Really Cool Packet for Trying-Out for UMBC's Collegiate Cybersecurity Competition Team aka CyberDawgs

UMBC CyberDawgs Team
Version (1738) // Revision (70.0.1)
Last Edited: Spring 2025

Table of Contents

Really Cool Tryout Packet

Step 0: Welcome

Hello! Welcome to the CyberDawgs Team tryouts.

Glad you could make it!

Below, you will find the Tryout Schedule, a step-by-step guide to help you navigate what to do next and help you pace yourself. While you are not being timed, you are limited to 3 total hours, so we suggest you strike a balance – be thorough, but don’t dawdle.

You are welcome to take a break, get a drink, go to the restroom, etc., at any time. Remember, though, that there is a hard stop for tryouts.

So that distractions and disturbances can be maintained at the lowest possible levels, please keep talking to a minimum. Instead, use Discord.

Please use your assigned channel in the Tryouts discord to communicate with the facilitators.

Tryout Schedule

Step 1.	**In-brief**	5 minutes
Step 2.	**Access & Guidelines**	5 minutes
Step 3.	**Initial Assessment**	50 minutes
Step 4.	**Take a Break (Recommended)**	5 minutes
Step 5.	**Incident Response**	45 minutes
Step 6.	**Security Recommendation**	40 minutes
Step 7.	**Out-brief**	5 minutes

Total estimated time:	150 minutes
Total allowed time:	180 minutes

Step 1: In-brief

Selection Criteria

Many different things are considered before inviting someone to join a CyberDawgs competition team. In addition to considering cybersecurity knowledge, prior competition experience, and cyber community experience, selecting individuals for a cyber competition team involves evaluating various soft skills and non-technical abilities. These include but are not limited to attention to detail, emotional intelligence, dedication, and the ability to follow instructions, to take direction, and to respect the chain of command. There are also a few different team goals that we hope to promote. Overall, we place the most importance on communication and group cohesion. Therefore, your ability to commit your time and efforts to the team is also an important consideration.

Historically, competing players have been talented, high-achieving individuals who are often involved in multiple clubs, scholar programs, volunteer work, traditional sports teams, employment, research, and academic pursuits. Issues should only arise if you miss enough team meetings to be out of the loop or are otherwise unprepared for a competition due to your other priorities.

In terms of minimum commitment, we want to emphasize the importance of self-motivation, a learning mindset, and practicing independently, as this dedication contributes significantly to the team's success. Outside of your time commitment, we understand that everyone is at least a part-time student, so we typically avoid scheduling activities during classes. That said, please note that joining the team may mean you need to miss a day or two of courses for these competitions. However, as a university-sponsored intellectual sports team member, you will receive excused absences for those dates.

Finally, while participation in the team's social aspects is not mandatory, we warmly encourage you to embrace every part of being a team member and look forward to having you actively involved. Cohesion is important, and it is important to get to know your teammates. If you proceed with the tryout today and receive an offer to join a team, we will follow up with more information.

Step 2: Access and Guidelines

Now, to get started! In your application, you indicated the operating system you were most comfortable with – you'll be assigned this operating system for the tryouts.

Windows users have been assigned a **Windows Server 2019** virtual machine.
Linux users have been assigned an **Ubuntu Server 18.04** virtual machine.

You will have two boxes for tryouts, of either Windows or Linux: an initial assessment box, where you are to find and report vulnerabilities and misconfigurations, and a breached box, a compromised version of the initial assessment box. You will not gain access to the breached box until after an initial assessment report is submitted.

Rules of Engagement

✔ You are allowed to use your notes and other materials
✔ You are allowed to freely access the internet (inclusive of AI)
✔ You are allowed to use publicly available open-source scripts/programs
✔ You are allowed to download/install programs to your tryout box
❌ Do not make any system configuration changes to your tryout box
❌ Do not harden or secure your tryout box
❌ Do not seek outside help. The tryout tasks must be done solely by you

At times, you may experience technical difficulties or want clarification. That's okay! While we will not guide you through the tryout beyond this document, you are welcome to ask any clarifying questions you may have at any time.

So that distractions and disturbances can be maintained at the lowest possible levels, please keep talking to a minimum. Instead, use your assigned channel in the Tryouts discord to communicate with the facilitators.

Step 3: Initial Assessment

After you access your tryout box, you might notice that it's not configured correctly. This is okay! Now, you can explore how the box is misconfigured and vulnerable and show us what you find. You perform an initial assessment and then write a vulnerability report.

Don't make any system configuration changes!

Make sure that whatever you do during your initial assessment doesn't change the current state of your machine, its settings, or configurations. If you so choose, you can run programs on the box, install new programs, run scripts, and look around. Be mindful of your time. **Do not remove anything from nor change anything on the box.** For example, do not change user passwords or permissions.

Notes: Consider keeping a few personal notes about features of the box, such as installed services, names of users, etc.

Be sure to include:

1. what the misconfiguration is
2. how did you discover the misconfiguration
3. why do you consider it a misconfiguration
   (i.e. say how it can be taken advantage of)

There is no strict format for writing your vulnerability report. Your communication style is your own. The following is only an example of the minimum information you should include.

Example Vulnerability Report Entry

Entry #02: There are no firewall rules implemented. I found this by opening Windows Defender and saw that there were no Inbound or Outbound rules listed. This means anyone can connect to the box through any open port.

As a Reminder: You must submit your report through Discord in your channel. Once your report is submitted, you will lose access to this machine and can move on to the Incident Response portion.

Step 4: Take A Break (Recommended)

Once you have completed your initial assessment and submitted your vulnerability report, you should take a break before continuing to Incident Response.

Step 5: Incident Response

Oh no! Your machine has been compromised. It happens. This is truly an inevitability in the real world. Now, you can demonstrate that you know what evidence (Indicators of Compromise) attacks can leave behind by identifying the changes made on your box and the exploits taken advantage of.

Continue not to make any system configuration changes!

Do not make changes to any system settings. Again, you can run programs, install programs, run scripts, and look around. Make sure that whatever you do doesn't change any settings or configurations. **You can add to the box; do not remove anything from or change anything on the box.**

Important note: You don't need to worry about resolving the issues created by the assumed breach. You're just here to investigate the incident. Your task is to report to us what actions were taken during the breach and how you identified the actions. Also, mention the security consequences or implications of what you found.

Example IR Report Entry

> Entry #08: There is a new connection listening on port 4311. I found this by running "sudo netstat -tulpn | grep LISTEN". This could be a backdoor that a malicious actor can use to regain access to the system.

As a Reminder: You must submit your report through Discord in your assigned channel.

Step 6: Security Recommendations

Almost done! At this point, you've performed an initial assessment of your system and responded to an incident where it is assumed your box was breached. Now, you will tell us how you would fix up the system you’ve been assigned.

We encourage you to review your original pre-breach vulnerability report and post-breach incident response report documents to refresh your memory about which misconfigurations and vulnerabilities exist. When writing your security recommendations, include commands, tools, or utilities you would employ to make your suggested changes.

Reminder: We don’t want you actually to secure the box. It would simply take too much time if we asked you to do that and document it all, and then we would need to check both the box and your report to validate your mitigations. Instead, we ask that you briefly explain your recommendations for securing the system.

Example Security Report Entry

> Entry #18: Update the password policy (with the Local Group Policy Editor - gpedit.msc) so users are required to use a complex password. This can mitigate the insecure password policy (#04 from the initial assessment).

As a Reminder: You must submit your report through Discord in your assigned channel.

Step 7: Out-brief

Congratulations! You did it!

We hope your tryout experience was fun, challenging, and not too stressful.
Sorry, you didn’t get to fight any bad guys this time!

Now that you’ve submitted all three reports pack up your stuff.
Then, hand in your tryout packet.

We will join you outside the room for a very quick out-brief.

Thank you for coming!